Method, apparatus and system for biometric authentication of a person

Background Of The Invention

The present invention relates in general to authentication of a person by detecting individual biometric features of said person and comparing them with corresponding, previously stored biometric features of the same person. In particular, the invention relates to a method for biometric authentication of a person, an apparatus used in this connection - for example a data carrier such as a smart card, etc. - and a system comprising such an apparatus and devices for detecting and comparing the biometric features.

For biometric authentication, a person's biometric features, for example a fingerprint, are checked by detecting the biometric feature and comparing it for sufficient similarity with a previously stored biometric feature. Positive comparison grants said person access to data, admission to rooms and similar measures protected from unauthorized access. The biometric features stored as reference data can be stored in any apparatus, for example a fingerprint door opener, or be portable by being stored in a smart card such as a money card, credit card, ID card and the like.

Biometric data can usually not be determined in precisely reproducible fashion, so that a match of stored reference data with currently measured comparative data is virtually impossible. For this reason the result of comparison is fixed as already positive if the match of the compared data exceeds a general threshold value, for example if only a 50 percent match is ascertained.

A disadvantage here is that the detection quality of biometric features varies from person to person. For example, the measuring result of a fingerprint is worse in the case of dry skin or very moist skin. Therefore, the threshold value is usually set altogether very low in order to be permit reliable authentication of all persons. However, a low threshold value simultaneously means a low security standard for access-protected facilities.

Summary Of The Invention

The problem of the present invention is therefore to provide a method, apparatus and system for more reliable biometric authentication.

This problem is solved according to the invention by the features of the independent claims. Advantageous embodiments of the invention are stated in the subclaims.

WO 95/26013 A1 discloses a system for biometric authentication wherein not only a specific biometric feature is stored and evaluated but also a non-specific biometric feature. During evaluation it is first checked whether the specific biometric feature of a person to be authenticated matches the stored specific biometric feature. After a successful check the non-specific biometric feature is also checked. The check of the non-specific biometric feature is supposed to ensure that the person being checked is actually present in person at the check.

DE 196 48 767 A1 discloses a smart card having a sensor for detecting fingerprints. In addition, the smart card contains memories in which the features of a fingerprint detected by the sensor are stored for a later check upon the first use of the card.

The invention is based on the finding that authentication can be made more reliable altogether if the authentication process takes account of a parameter unique to each person which is determined with reference to this person's individual feature quality. For the biometric feature "fingerprint," for example, skin moisture is a quality factor. If the person in question has skin which is comparatively neither especially dry nor especially moist, the parameter for the individual feature quality is fixed at over 100 percent of a standard value, and in the case of especially moist or especially dry skin at a value under 100 percent of the standard value.

This increased or reduced individual parameter as an absolute deviation from the standard value can then be taken as a measure of the lowering of the individual threshold value over a standard threshold value. The standard threshold value can be fixed comparatively high, for example at 80 percent instead of the abovementioned 50 percent. The individual threshold value is then in the range of 50 percent to 80 percent depending on the individual feature quality. This accordingly impedes imitation of the biometric feature, thereby likewise increasing the security of the system.

Alternatively, the parameter for the individual feature quality, once determined, can be used to adjust the sensor system of a measuring instrument used for redetecting the biometric feature for the purpose of authentication. With capacitive measurement of the fingerprint, the quantity of electricity is increased over the standard setting in the case of suitable skin and accordingly reduced with less suitable skin.

Accordingly, it can be expedient to determine separate parameters for different properties influencing a certain person's feature quality, said parameters either being taken into account individually for adjusting the sensor system of a measuring instrument or entering a threshold value individual for this person. A combination of these two measures is also possible.

B Detailed Description of The Invention

The inventive method works as follows. First, a person's biometric data, for example a fingerprint, are detected and stored as reference data. The data can be stored for example in a first memory area of a data carrier, for example smart card. Said reference data are usually detected in a secure environment and under the instruction of experienced technical personnel. During this phase of reference data detection, user-unique information on the quality of the biometric feature is additionally determined and stored in a second memory area. The user-unique information can be for example

the moisture of the skin or a similar individual property of the person in question relevant to the biometric feature. This information about the individual feature quality serves as a parameter in the following verification phase.

In the verification phase, the same biometric feature of the person in question is redetected and converted into biometric data which are compared with the biometric feature stored as reference data in the first memory area. This comparison leads to a match of regularly under 100 percent. Whether this match suffices for authentication depends on whether a predetermined threshold value is exceeded, said value in turn depending on the parameter stored in the second memory area. If the person in question has average skin moisture, for example, the stored parameter has a value of 100 percent. The threshold value is accordingly adjusted to the highest average threshold value. The average threshold value can be adjusted for example to an 80 percent match, so that in the present case authentication only takes place if the match is at least 80 percent. With especially suitable or especially unsuitable skin, the parameter would be for example 120 percent or 80 percent and the associated threshold value accordingly lower, so that authentication already takes place at a 64 percent match, for example.

The parameter can be used alternatively or additionally to adapt the sensor system for redetecting the biometric data in the verification phase to the person's individual feature quality. As mentioned at the outset, the quantity of electricity of a capacitive fingerprint sensor would be increased (e.g. by 16 percent) over the standard setting according to the parameter (e.g. 120 percent) in the case of suitable skin, and accordingly reduced (e.g. to 64 percent) in the case of less suitable skin (parameter 80 percent).

In a further embodiment of the invention it is provided that the possibilities of activity granted the person after successful authentication are limited ("activity filter"), e.g. it can be provided that a maximum amount is stipulated for financial transactions. The limitation is performed either if this person's individual feature quality is bad by nature, i.e. the stored parameter deviates from the standard value, or if the individual feature quality is basically good but the comparison between the stored reference data and the currently detected biometric data is only slightly above the associated, individ-

ual threshold value. In both cases there is a comparatively great danger that the redetected biometric data were manipulated.

A further advantageous embodiment of the invention provides that the sensor system for redetecting the biometric data during the verification phase is adapted in such a way that roughly the same measuring results are always achieved independently of the particular environmental conditions. For example, the quantity of electricity can be adjusted in dependence on the humidity in the case of capacitive fingerprint sensors. Environmental influences vary constantly in different places (e.g. bank branches) and at different times of the day or year. The above-described measure can therefore make authentication more reliable in the end. Other environmental influences are for example the lighting conditions, temperature, etc. Such influences can be taken into account by adjusting a camera with respect to film speed, for example, or electrically heating a capacitive sensor chip for detecting the fingerprint. It is especially advantageous if the sensor system is adapted to the environmental conditions prevailing in the phase of reference data detection. For this purpose the environmental conditions prevailing during reference data detection are stored in a third memory area so that they are available together with the individual parameters and reference data.